ОТЗЫВ

на автореферат диссертации Прудникова Вадима Александровича выполненной на тему «Синтез и исследование псевдо-динамических подстановок» и представленной на соискание ученой степени кандидата технических наук по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертационного исследования

Операции замены или фиксированные подстановки sbox являются основным нелинейным элементом для множества современных псевдослучайных функций (Pseudo Random Function – PRF) и псевдослучайных перестановок (Pseudo Random Permutation – PRP), которые являются базовым элементом логической защиты информации в информационных системах. Под термином «подстановка» (sbox, замена) подразумевается как взаимно однозначное, так и не взаимно однозначное преобразование m-битного сообщения на входе в n-битное сообщение на выходе, где n не всегда равно m.

Нелинейность подстановок напрямую влияет на сложность криптоанализа псевдослучайных функций и псевдослучайных перестановок, операции замены являются одним из наиболее ресурсоёмких элементов при программной или аппаратной реализации. Так как PRF и PRP строятся по итеративной схеме (для достижения заданного уровня суммарной нелинейности преобразования), от нелинейных свойств фиксированных подстановок напрямую зависит количество итераций, затрачиваемых вычислительных ресурсов, а также время обработки и потребляемая мощность.

К фиксированным операциям подстановки предъявляется около десятка требований, напрямую влияющих на криптографическую стойкость PRF и PRP. Для малоресурсных псевдослучайных функций и псевдослучайных перестановок остро встаёт проблема защиты от побочных каналов утечки секретной информации. Это накладывает дополнительные требования и ограничения на подстановки.

Актуальность исследований заключается в том, что проблема синтеза подстановок, удовлетворяющих широкому спектру взаимоисключающих требований, является базовой при синтезе эффективных PRF и PRP. Псевдослучайные функции, работающие в режиме счётчика с аутентификацией Галуа (Authenticated Encryption with Associated Data – AEAD), в большинстве случаев способны заменить современные блочные шифры, например, в протоколах SSH и TLS, а также OpenVPN, так как обладают более высокой производительностью и/или меньшим потреблением ресурсов при программной реализации. Однако применение псевдо-динамических подстановок при синтезе PRF потенциально способно обеспечить устойчивость к криптоанализу превосходящую аналоги, при сохранении сопоставимых затратах ресурсов при программной реализации. Следовательно, синтез и исследование псевдо-динамических подстановок является актуальной темой и представляет научный и практический интерес.

Оценка достоверности полученных результатов и новизны диссертационного исследования

Достоверность результатов и обоснованность научных положений, результатов и основных выводов диссертационной работы подтверждается

сходимостью исходной гипотезы с результатами опытно-экспериментальных данных, а также строгостью применяемого математического аппарата.

Научная новизна состоит в следующем:

1. Разработана структура псевдо-динамической операции подстановки на основе ARX-функций, обладающая свойствами эквивалентных замен, аналогичными случайно сформированным операциям подстановки той же размерности (пункт 19 паспорта специальности).

2. Разработан и исследован метод синтеза параметров 32-битной ARX-функции, позволяющий получить параметры операций циклического сдвига, при которых обеспечивается максимальный вес разностной характеристики, равный 2^{-32} (эмпирический вес 2^{-26}), и вес линейной характеристики 2^{-13} для результирующего PD-sbox-ARX, включающей в свой состав четыре 32-битные ARX-функции, а также позволяющий минимизировать количество затрачиваемых ассемблерных инструкций на операции циклического сдвига при реализации на малоресурсных 8-битных микроконтроллерах семейства AVR (пункт 19 паспорта специальности).

Теоретическая значимость полученных результатов

Теоретическая значимость результатов исследования состоит в развитии перспективного научного направления синтеза и применения псевдо-динамических подстановок на основе ARX-функций, удовлетворяющих широкому спектру противоречивых требований по стойкости к криптоанализу и затрачиваемым ресурсам при программной реализации криптографических преобразований.

Практическая ценность полученных результатов

Применение псевдо-динамических подстановок на базе подобранных ARX-функций, обладающих дифференциальными и линейными свойствами эквивалентных подстановок, аналогичными случайно сформированным фиксированным подстановкам той же размерности, позволяет обеспечить критический путь (максимальное количество последовательных операций сложения по модулю 2^{16}) в четыре раза меньше, чем 8-итерационная 32-битная Alzette-подобная структура, при двухкратном увеличении количества операций и при сопоставимых максимальных значениях весов разностных и линейных характеристик. При аппаратной реализации ARX-функции данное свойство позволяет пропорционально уменьшить (до 4 раз) задержку при преобразовании блоков информации.

Публикации, отражающие основное содержание диссертации

Основные положения диссертации опубликованы в 11 научных печатных работах, в том числе: 5 – в ведущих рецензируемых научных журналах, входящих в перечень ВАК РФ (из них 1 категории К1 и RSCI, 4 категории К2), 6 – в материалах конференций и других изданиях. Получено свидетельство о государственной регистрации программы для ЭВМ.

Замечания и рекомендации

1. В тексте автореферата отсутствует криптографическое определение термина «Эквивалентная замена».

2. Из текста автореферата следует, что анализ потребляемых ресурсов сфокусирован только на инструкциях для ROL (циклического сдвига). Несмотря на

то, что это важный фактор для микроконтроллеров архитектуры AVR, полная оценка количества используемых инструкций должна включать и другие операции (ADD, XOR). Последнее не нашло отражение в тексте.

Несмотря на отмеченные замечания, судя по автореферату, диссертация выполнена на требуемом научно-техническом уровне и соответствует научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Диссертация Прудникова Вадима Александровича «Синтез и исследование псевдо-динамических подстановок» удовлетворяет требованиям, установленным Положением «О присуждении учёных степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет» (в действующей редакции) и предъявляемым к диссертациям на соискание учёной степени кандидата наук, а автор, Прудников Вадим Александрович, заслуживает присвоения ему учёной степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность», технические науки.

Лепешкин Олег Михайлович, доктор технических наук, доцент.
Российский государственный гидрометеорологический университет профессор кафедры информационных технологий и систем безопасности.

195027, г. Санкт-Петербург, проспект Металлистов, д. 3, лит. А
lepechkin1@yandex.ru, тел. +79052851649.

02.06.2025

Подпись Лепешкина
ФИО Олега Михайловича
ЗАВЕРЯЮ
Начальник управления кадров
Подпись
Расшифровка Н.Д. Соколова
Управление кадров